# Methods of Proof

Zach Wagner
Department of Mathematics
University of California, Los Angeles
Los Angeles, California 90024 USA

August 15, 2012

**Abstract**

Of all of the subjects encountered when studying mathematics, none are more intimidating than the rigorous proof. Proofs are what mathematics is based on; in fact, mathematics relies on the notion of completely correct and well written proofs that flow methodically and logically. Such can be a difficult feat for prospective mathematics undergraduates that have had little or no exposure to proof writing. In this paper, we summarize a few fundamental methods of proof.

# 1 Introduction

We assume the reader is familiar with most elementary mathematical subjects, from linear algebra to general calculus (single and multivariable). To understand the underlying logic of proofs requires a thorough course in mathematical logic. Here, we assume no such prior experience and jump right into some fundamental methods of proof.

It goes without saying that a basic understanding of set theory is required for anyone to prove *anything*! Let $A$ and $B$ be arbitrary sets. We say that,

$$A = B$$

if and only if $A \subseteq B$ and $A \supseteq B$. Furthermore, we say that,

$$A \subseteq B$$

if and only if, for any $x \in A$, $x \in B$. By the **union** of a collection of sets, we mean that, for any $x$ in this union, $x$ appears in at least one set in the collection. We write,

$$\bigcup_{n \in I} A_n$$

for a collection of sets $\{A_n\}$ and some index set $I$. For instance, $I$ could be the natural numbers up to some $N$, in which case the union is taken over all $n = 1, 2, ..., N$. Let $A$ be this union. Then $x \in A$ implies that $x \in A_i$ for some $i \in I$. This is merely a redundancy of what was stated above, but we used mathematical language, as you should in your proofs.

By the **intersection** of a collection of sets, we mean that, for any $x$ in the intersection, $x$ appears in all sets in the collection. We write,

$$\bigcap_{n \in I} A_n$$

with all notation as described above. Notice that $x \in A$ for $A$ being the intersection implies that $x \in A_i$ for all $i \in I$. To see how this all works together, consider the following.

**Theorem 1.1.** *Let A,B, and C be sets. Then,*

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

*Proof.* We first prove,

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C) \tag{1}$$

Let $x \in (A \cup B) \cap C$. Then $x \in A \cup B$ and $x \in C$. If $x \in A \cup B$, then $x \in A$ or $x \in B$. In either instance, $x \in A$ and $C$ or $x \in B$ and $C$. This proves (1). We now prove that,

$$(A \cup B) \cap C \supseteq (A \cap C) \cup (B \cap C) \tag{2}$$

Letting $x$ be in the right side, we see that $x \in A$ and $C$ or $x \in B$ and $C$. In both cases, $x \in C$, so we notice that we are only concerned with $x \in A$ or $x \in B$. In this case, $x \in A \cup B$, so $x \in (A \cup B) \cap C$. This proves (2). The theorem follows.

□

Understanding this, we now proceed to summarize some methods of proof.

## 2 Direct Proof

**Theorem 2.1.** *Let $V$ be a vector space over a field $F$. Let $W_\alpha$ be a collection of subspaces of $V$ with $\alpha \in I$ for some index $I$. Then,*

$$\bigcap_{\alpha \in I} W_\alpha \tag{3}$$

*is a subspace of $V$.*

*Proof.* To prove that (3) is a subspace, it suffices to show closure under addition and scalar multiplication. Let $x, y$ be elements of (3) and let $c \in F$. Then $x, y \in W_\alpha$ for all $\alpha$. But each $W_\alpha$ is a subspace, so $cx + y \in W_\alpha$ for all $\alpha$. This implies that $cx + y$ is in (3). Thus, the intersection is a subspace of $V$. Done.

□

## 3 Contradiction

**Theorem 3.1.** $\sqrt{2} \notin \mathbb{Q}$. *That is, $\sqrt{2}$ is irrational.*

*Proof.* Suppose $\sqrt{2}$ is rational. Then for some relatively prime $p, q \in \mathbb{Z}$, we have,

$$\sqrt{2} = \frac{p}{q}$$

In other words, $\frac{p}{q}$ is in lowest terms. But notice,

$$2 = \frac{p^2}{q^2}$$

Hence, $2q^2 = p^2$. This shows that $p^2$ is even, so $p$ is even. Thus, write $p = 2k$ for $k \in \mathbb{Z}$. Then $2q^2 = 4k^2$, so $q^2 = 2k^2$. Hence, $q$ is even. Since both $p$ and $q$ have a factor of 2, this contradicts the notion that $\frac{p}{q}$ is in lowest terms.

Hence, what we assumed is false and $\sqrt{2} \in \mathbb{Q}$.

□

**Remark:** Remember that contradiction may be a good choice when the consequence of a proof is a "black and white" statement. Here, for instance, a number is either rational or it isn't. In the previous proof in the "Direct Proof" section, it may not be so easy to prove the theorem if you assume that the intersection is not a subspace (for, if not, what is it??). Contradiction is tempting to use and you should avoid getting in the habit of turning to it first for any proof.

Also, remember that when you choose to use proof by contradiction, you *must* show how you used the negation of the consequence. What I commonly see people do is proceed via "contradiction," but then they just use direct proof. They see this as a contradiction because the consequence obviously contradicts the negation of the consequence. But they failed to show how the negation of the consequence results in some fundamental mathematical flaw. Take caution with this.

## 4 Induction

This next theorem is really a very silly example of induction, but it shows how all of the steps work. The result after this next theorem is from the textbook and demonstrates induction in a slightly less trivial way.

**Theorem 4.1.**

$$\sum_{i=1}^{n} n = \frac{n(n+1)}{2}$$

*Proof.* First, assume $n = 1$. Then $1 = \frac{1(1+1)}{2} = 1$. Hence, the first case (”base case”) holds. Assume that the theorem holds for $n$ and consider $n+1$. Well, the $n+1$ sum is,

$$\sum_{i=1}^{n+1} n$$

But this is,

$$n + 1 + \sum_{i=1}^{n} n$$

By the induction hypothesis, we have,

$$n + 1 + \frac{n(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Thus, the $n+1$ case holds as expected. The theorem therefore follows by induction. □

**Theorem 4.2.** *If $W$ is a subspace of a vector space $V$ and $w_1, ..., w_n$ are in $W$ for arbitrary $n$, then,*

$$\sum_{i=1}^{n} a_i w_i \in W \tag{4}$$

*for any $a_1, ..., a_n \in F$ (the field).*

*Proof.* If $n = 1$, then we simply have that $w_1 \in W$. Since $W$ is a subspace, then by definition, $a_1 w_1 \in W$. Suppose then that (1) holds for $n$ and consider $n+1$. Then we want to show that,

$$\sum_{i=1}^{n} a_i w_i + a_{n+1} w_{n+1} \in W \tag{5}$$

But by assumption, $\sum a_i w_i \in W$. Also, by similar reasoning to above, since $W$ is a subspace, $a_{n+1}w_{n+1} \in W$. Finally then, let $\sum a_i w_i = v$. Then since $v \in W$ and $a_{n+1}w_{n+1} \in W$, since $W$ is a subspace, $v + a_{n+1}w_{n+1} \in W$. Ergo, (2) holds. This is enough to show (1) by induction.

□

# 5 Final Note

Please bear in mind that these are only examples of the vast power these methods of proof have. Also, I neglected to show another method of proof (my personal favorite!): contrapositive. As contrapositive is a bit of a mess with logic, I will leave this to your Professor. You likely won't need it much anyway for 115A.